Chapter

3

Azure Core Networking Services

MICROSOFT EXAM OBJECTIVES COVERED IN THIS CHAPTER:

DESCRIBE CORE AZURE SERVICES

✓ **Describe core resources available in Azure**

- Describe the benefits and usage of Virtual Networks, VPN Gateway, Virtual Network peering, and ExpressRoute

The previous chapter explored several core Azure architectural components and core Azure services, with a focus on compute, data, and storage services. This chapter continues coverage of Azure core services focused on networking. A good grasp of these core networking services will not only help you understand how some of the other core services connect with one another, but will also prepare you to dive into security aspects of Azure, which are covered in Chapter 4, "Security, Compliance, Privacy, and Trust."

Networking Concepts

The Azure Fundamentals exam is not just for deeply technical roles—sales professionals, power users, solution specialists, and other less technical roles can benefit from a fundamental understanding of Azure. If you are in a role that is not deeply technical, you might not understand networking concepts sufficient to the requirements of the AZ-900 exam. This section lays the groundwork for the remainder of the sections in this chapter by covering some basic networking concepts. If you are a technical professional, you can skip this introductory section.

Client-Server and Serverless Computing

Until relatively recently, a *client-server* model prevailed in IT, with discrete servers hosting applications and services that were consumed by client systems (like desktop, notebook, and mobile devices). The servers were either physical or virtual. That model is still the most common, but as described in Chapter 1, "Cloud Concepts," PaaS and SaaS cloud offerings are evolving the way services are delivered to clients. In addition to discrete servers hosting applications and services, *serverless computing* means that the server is abstracted (or essentially hidden from the service consumers) and the service becomes the primary focus. Azure SQL Database is a great example. When you need a SQL database, you simply provision one and Azure handles all the server-related resources on the back end without any intervention from you.

Regardless of the model your solutions use, the servers, serverless applications, and clients need a way to communicate with one another. Networks provide that means of communication. For example, your email application needs to know where to find the mail server so that it can send and receive your email. Your web browser needs to turn a web address like `www.microsoft.com` into something that enables it to send requests to and receive responses back from the web server. Network addressing and the Domain Name System (DNS) are the primary mechanisms that make that communication possible.

Network Addressing

Each device on a network, whether physical or virtual, needs a unique identification that enables other devices and services to communicate with it. Each device is assigned a *network address* that serves as its address, much like a street address identifies the place where you live. For the AZ-900 exam, you don't have to understand network addressing in detail, so for now, think of a network address space as describing the building addresses in a specific neighborhood. Within that network address space, *subnets* further segregate parts of the address space into virtual networks. Using the neighborhood analogy, think of the subnet as describing a specific street in the neighborhood.

> **TIP**
>
> The two network address protocols used today to route traffic across local networks and the Internet are IPv4 and IPv6. The IP in the names stands for Internet Protocol. IPv4 uses a four-octet address to uniquely identify devices, such as 192.168.0.107. IPv6 uses eight groups of hexadecimal digits separated by colons, such as 0:0:0:0:0:FFFF:C0A8:006B.

Your personal computer (and other network devices including your mobile phone) receives a network address when it boots. The mechanism of how that works is not relevant to this discussion, but understand that the address identifies your device uniquely on its network. The address is defined by the network address space and a *subnet mask* that defines the virtual network on which your device resides.

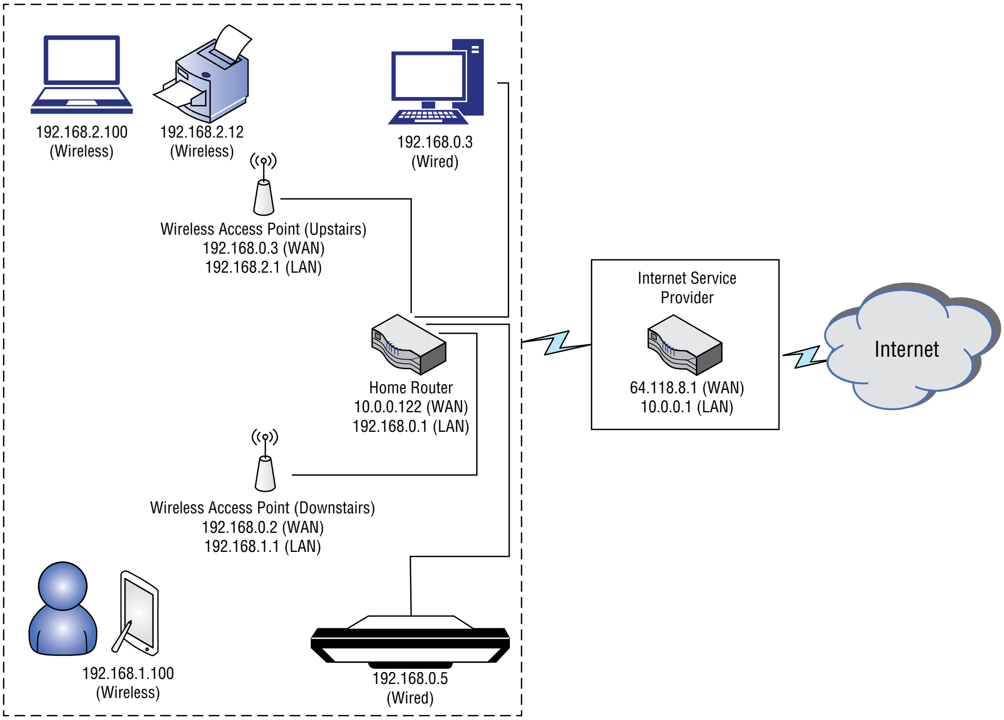
If you are connected to a home Wi-Fi network, for example, your device is assigned an address from your Wi-Fi access point and the network uses that address to route traffic (information) to and from your device. Other devices on the network can also use that address to communicate with your device. For example, when you print a document to a network-connected printer, that data is routed from your network address to the printer's network address. Figure 3.1 illustrates an example of a home network.

Computers and other devices have no problem using numbers for addresses, but people do. That is where the Domain Name System comes into play.

Domain Name System

The Domain Name System (DNS) maps numeric IP addresses to *hostnames* that are more easily recognized and understood by people. For example, DNS maps the hostname `www.microsoft.com` to an IP address of 23.35.205.40. So, when you want to visit the Microsoft website, you type **`www.microsoft.com`** into your web browser instead of the numeric address. A *DNS resolver* on your computer communicates with a DNS server whose job it is to look up addresses associated with hostnames and return the hostname to your web browser. It is a bit like asking a directory service, “What’s the street address for Joseph Q. Brown in Fargo, North Dakota?”

FIGURE 3.1 A simple home network



DNS is complex, but a deep understanding of how it works is not necessary to understand the topics in the AZ-900 certification exam. The key point is that client applications communicate with DNS servers to obtain the IP addresses associated with hosts like web servers, database servers, printers, and other network resources. The client applications then communicate with those hosts using their IP addresses. Likewise, servers and server applications communicate with one another using IP addresses that they obtain by looking up the address from a DNS server.

TIP

One key DNS topic to understand for the exam is denial-of-service (DoS) attacks, in which an attacker floods a system with traffic to overwhelm it and prevent it from functioning. Chapter 4 discusses DoS attacks that target DNS.

Routing

Earlier in the section "Network Addressing," you learned that networks are segmented into subnets (subnetworks), much like buildings are organized by their street. Your home network is a simple example of a network subnet. Figure 3.1, shown previously, illustrates a typical home network that includes a 192.168.0.x subnet for wired devices, a 192.168.1.x subnet for one Wi-Fi network, a 192.168.2.x segment for another Wi-Fi network, and a 10.0.0.x network for the Internet service provider (ISP).

The wireless access points (WAPs) in Figure 3.1 function as *routers*, routing data between the two subnets that they host and the local network. The home router handles traffic between those WAPs and the ISP's network. The ISP's router handles traffic to the Internet. For example, when you open a web page on your wireless tablet, the WAP manipulates the address information before sending it on so that the next router up the chain knows where to send the response. The next router does the same thing until the data reaches the web server. Then, the process is reversed until the data gets back to your WAP, which sends the response to your tablet.

NOTE

Address translation and the other aspects of routing are complex and well outside the scope of this book. The key point to understand is that routers move data between subnets, manipulating the data so that the traffic can reach its intended destination and responses can come back to the requesting system.

TIP

There are two types of subnet—private and public. A private subnet is one that does not have a presence on the Internet. Your home Wi-Fi network is an example of a private subnet. Because it is private, that same subnet can be used by your neighbor. Your subnet is hidden from the Internet by your router. Public subnets have a presence on the Internet and corresponding host entries in the DNS system. Think of it this way: strangers know how to get to your home address because it is public but do not know where the television is in your home. The router is like a director at your front door who directs traffic intended for your television.

The main point to understand for the AZ-900 exam is that servers and services in Azure need IP addresses to route data. As with your home network, your subnets in Azure are private subnets, but at the point where your Azure networks meet the Internet, you have public network addresses. The public addresses are owned and managed by Microsoft, and the private addresses are assigned and managed by you.

Virtual Networks

A core concept for Azure and for any networking discussion is *virtual networks*, and the Azure Virtual Network (VNet) service is a fundamental component of your private Azure networks. VNet enables virtual machines and other Azure services to communicate among themselves, with the Internet, and in the case of a hybrid environment, with your on-premises networks. As you might expect from an Azure service, VNet adds availability and scalability to your network resources in Azure.

As you do with other Azure resources, you must create VNet resources in Azure. When you create a VNet, you specify the private IP address space that the VNet will use. Within that address space, subnets that you define enable you to segregate network segments for various resources. A virtual network is scoped to a single region and a single subscription. However, you can create multiple virtual networks within a region and subscription.

You can use virtual network peering to connect virtual networks, including across regions. This enables your resources to communicate across virtual networks (globally, if necessary), with the traffic traversing Microsoft's private backbone network. Resources in the peered virtual networks can communicate at the same latency and with the same bandwidth as they would if they were on the same virtual network.

Load Balancers

Load balancing refers to distributing network traffic across multiple resources to improve responsiveness, reliability, and availability. For example, if you deploy a web application with three web servers, you will use a load balancer to distribute the traffic among the three web servers. Client systems see a single hostname and IP address for the balanced services, and the load balancer distributes the traffic across the hosts in the balanced group. Not only does this distribute the load for performance reasons, but if one of the web servers fails, the load balancer can exclude the failed server from the group and begin sending all the traffic to the remaining two. Or, if you scale out with additional servers, the load balancer will begin sending traffic to the new servers.

Azure offers four load balancing services:

- **Azure Front Door:** Azure Front Door is designed for global or multiregion routing and site acceleration of Internet-facing web traffic. It uses the Microsoft global edge network to enable fast, secure, and scalable web applications.
- **Azure Traffic Manager:** This service is an application layer DNS-based traffic load balancer that balances traffic at the domain level. It can balance traffic across global Azure regions. Traffic Manager offers several options for routing traffic and detecting endpoint health.
- **Azure Application Gateway:** This is an application layer load-balancing service that provides an application delivery controller (ADC) as a service. You can configure Application Gateway as Internet-facing, internal-only, or a combination of the two. Azure Application Gateway is applicable for HTTP(S) traffic and can route traffic based on several criteria, including incoming URL, URI path, and host headers.

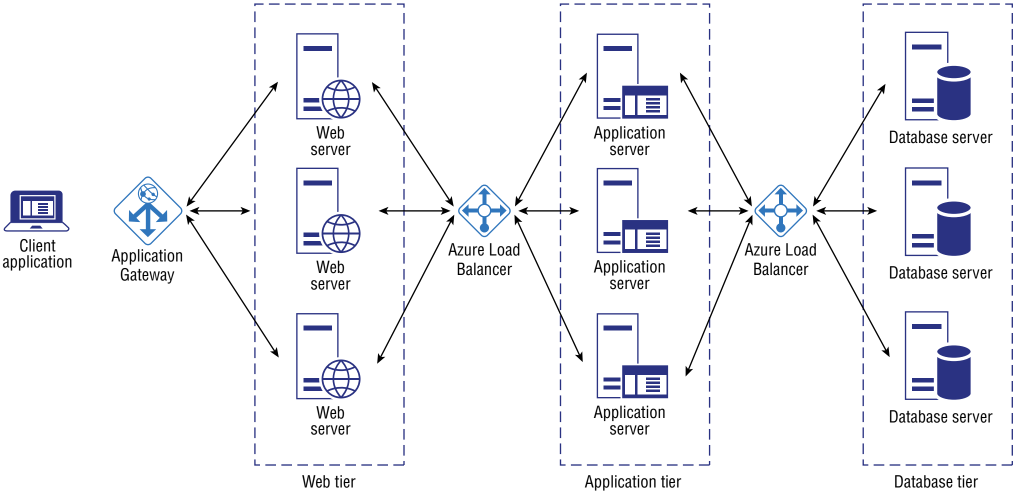
- **Azure Load Balancer:** The Azure Load Balancer service is a transport layer service designed for high performance and low latency and is zone-redundant to provide high availability across availability zones. It is applicable for non-HTTP(S) traffic.

NOTE

What do layers mean in the context of load balancing? The OSI model is a conceptual model created by the International Organization for Standardization (ISO) to enable communication between various systems. The OSI model encompasses seven layers: (1) physical, (2) data link, (3) network, (4) transport, (5) session, (6) presentation, and (7) application. The layers referenced in the discussion of the types of load balancers refers to the OSI layers. Azure Traffic Manager and Azure Application Gateway both function at layer 7, whereas Azure Load Balancer service functions at layer 4. A load-balancing service can support different functionality based on the level at which it functions. The OSI model and the details surrounding the layer-specific benefits are outside the scope of the AZ-900 exam.

Figure 3.2 shows an example of two Azure load-balancing services working together to balance traffic.

FIGURE 3.2 The load-balancing services in Azure can work individually or in concert, as in this example.



Which load-balancing service you choose depends on the scenario, and you might use one in some situations and more than one in others. Azure Load Balancer is generally the appropriate solution for non-HTTP(S) traffic based on the IP address of the target service. For example, you would use Azure Load Balancer when balancing traffic among multiple database VMs.

Azure Application Gateway is designed to support regional load balancing for HTTP(S) traffic and offers support for path-based routing. For example, assume you want to route traffic to a set of web servers. When the URL includes `/videos` in the path, you want to direct the traffic to a specific pool of servers that are optimized to handle video requests. Azure Application Gateway gives you that capability.

Like Azure Application Gateway, Front Door supports URL path-based routing. However, Azure Front Door is intended for globally distributed web applications where speed, user location, fast failover, caching, and high availability are critical. If you are configuring regional routing, think Azure Application Gateway. For global routing, think Front Door.

Azure Traffic Manager is appropriate for DNS-based global routing. Traffic Manager supports a variety of methods for routing traffic and for detecting endpoint health, enabling Traffic Manager to support a wide range of applications and usage scenarios where region or global load balancing is needed.

For the purposes of the AZ-900 exam, consider Azure Load Balancer as the service you would choose to balance traffic evenly across multiple virtual machines based on IP address. Application Gateway performs URL-based routing across multiple instances. Traffic Manager routes traffic to the data center that is geographically closest to the user. Front Door also provides that capability, but it offers additional features for global deployment of web applications.

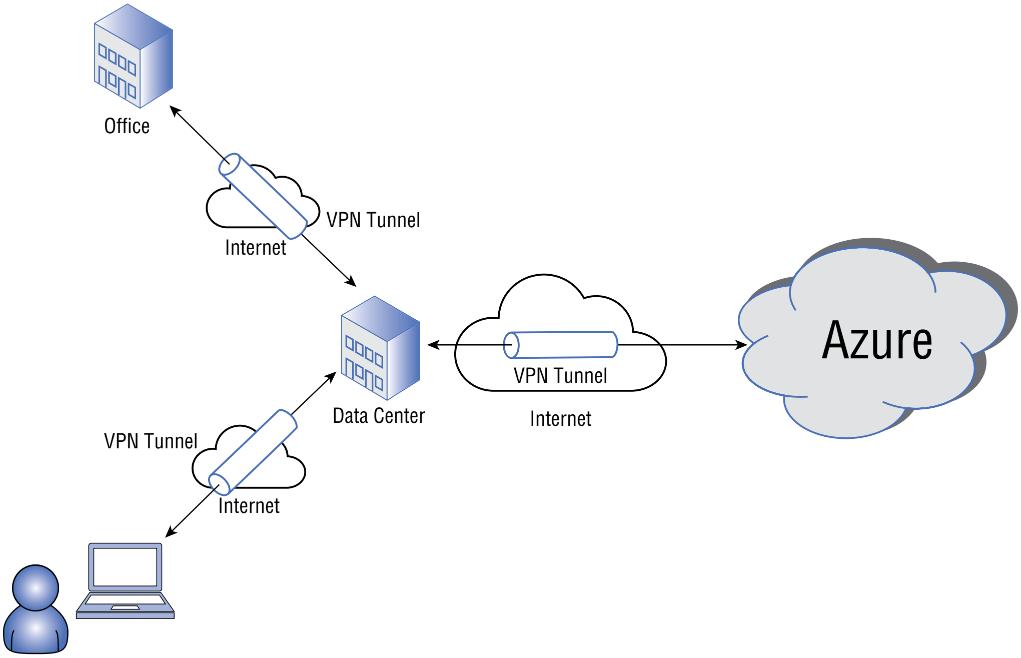
For details and recommendations on which service is most appropriate, see `https://docs.microsoft.com/en-us/azure/architecture/guide/technology-choices/load-balancing-overview`.

VPN Gateway

The section "Network Addressing" earlier in this chapter described network addresses and network segments. That section described a home network scenario that included a couple of private network segments. Imagine that you are working from home and need to access a web server at work that contains business-sensitive information. That data would be subject to compromise if it were traversing the public Internet, particularly if the traffic were not encrypted. Virtual private networks (VPNs) help solve that problem.

A VPN establishes an encrypted tunnel between two private networks across a public network. For example, you can establish a secure connection between your on-premises network and Azure using a VPN, enabling traffic to flow securely between your on-premises data center and your resources in Azure. Similarly, you can use a VPN connection between your home network and office network to access the web server that hosts that business-sensitive data, protecting the data from prying eyes as it travels between the server and your computer. Figure 3.3 illustrates VPN connections.

FIGURE 3.3 A VPN connection establishes a secure tunnel between networks.



Even if your organization hosts all its IT resources in Azure, you will certainly need a VPN connection between your users and Azure to ensure that traffic between client applications and the services that host them in Azure is encrypted and secure. One option for creating a VPN connection to Azure is to use the Azure VPN Gateway service, discussed next.

Azure VPN Gateway

Azure VPN Gateway enables you to create VPN connections between Azure virtual networks and between Azure and your on-premises network. VPN Gateway supports multiple VPN configurations:

- **Site-to-site:** Establishes a VPN tunnel between two sites, such as between your on-premises data center and Azure.
- **Multi-site:** A variation of site-to-site, a multi-site VPN establishes VPN tunnels between Azure and multiple on-premises sites.
- **Point-to-site:** Establishes a VPN tunnel from a single device (point) to a site.
- **VNet-to-VNet:** Establishes a VPN tunnel between two Azure VNets.

A site-to-site VPN connects two sites, such as an on-premises facility and Azure. For example, you might use a site-to-site VPN to connect your primary data center and Azure, enabling secure, encrypted traffic between the on-premises servers and services that interact with resources in Azure. Or you might use a site-to-site VPN to connect your primary office location to Azure to secure user-related data traffic between the office and Azure. A multi-site VPN provides an expanded site-to-site capability. For example, you might use a multi-site VPN to create a secure connection to Azure from separate data center and office locations.

A point-to-site VPN is similar to a site-to-site VPN in that it creates an encrypted tunnel, but the connection is between a single device and a site. If only one server or service at one of your locations needs to connect to Azure, you can use a point-to-site VPN to connect that one server to Azure.

A VNet-to-VNet VPN connects two Azure VNets with an encrypted tunnel. The VNets can be from different regions and subscriptions. Connecting VNets in this way enables you to connect resources and networks in different Azure locations without traversing the Internet. One common use for a VNet-to-VNet VPN is to enable georedundancy of services. Assume, for example, that you want to build a highly available SQL Server solution that uses SQL Server Always On to replicate databases between different regions in an availability group. A VNet-to-VNet VPN tunnel between the two regions where the virtual servers reside provides the connectivity needed for replication between those regions.

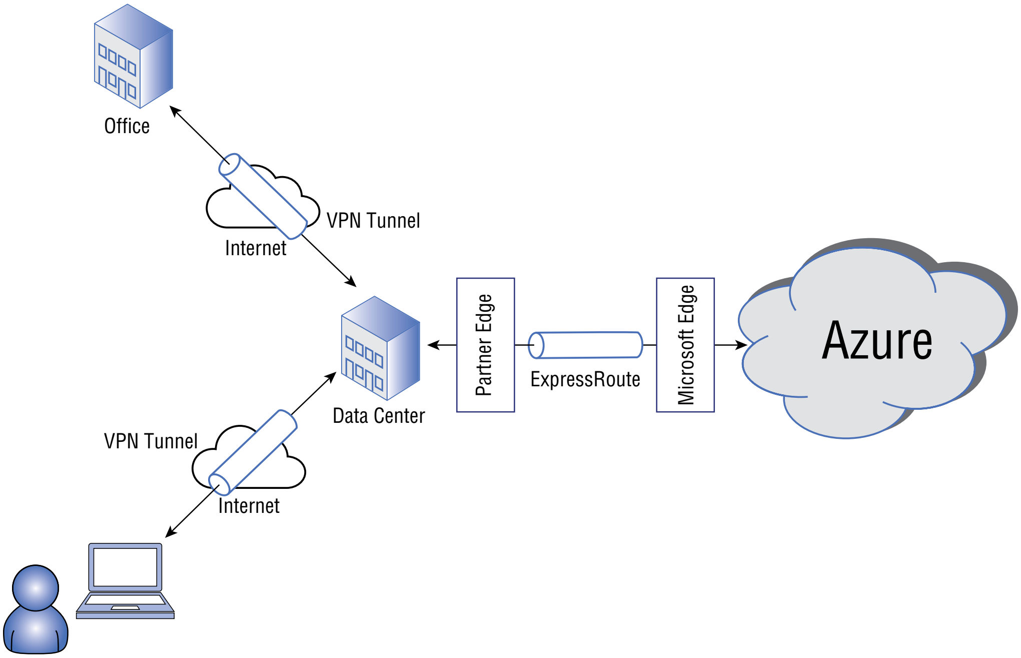
ExpressRoute

Azure ExpressRoute enables you to extend your on-premises networks into Azure over a private connection managed by a third-party connectivity provider. The route does not traverse the Internet, enabling higher reliability, faster speeds, less (and more consistent) latency, and higher security. Figure 3.4 illustrates an ExpressRoute connection.

TIP

ExpressRoute Direct, as an alternative to ExpressRoute, enables you to connect directly to the Microsoft global network without traversing the Internet. Consider ExpressRoute Direct if you require physical isolation as a regulated industry or government entity, or if you need to move massive amounts of data into Azure. See https://docs.microsoft.com/en-us/azure/expressroute/expressroute-introduction for more information on both ExpressRoute and ExpressRoute Direct.

FIGURE 3.4 ExpressRoute establishes a secure route from your on-premises network to Azure.

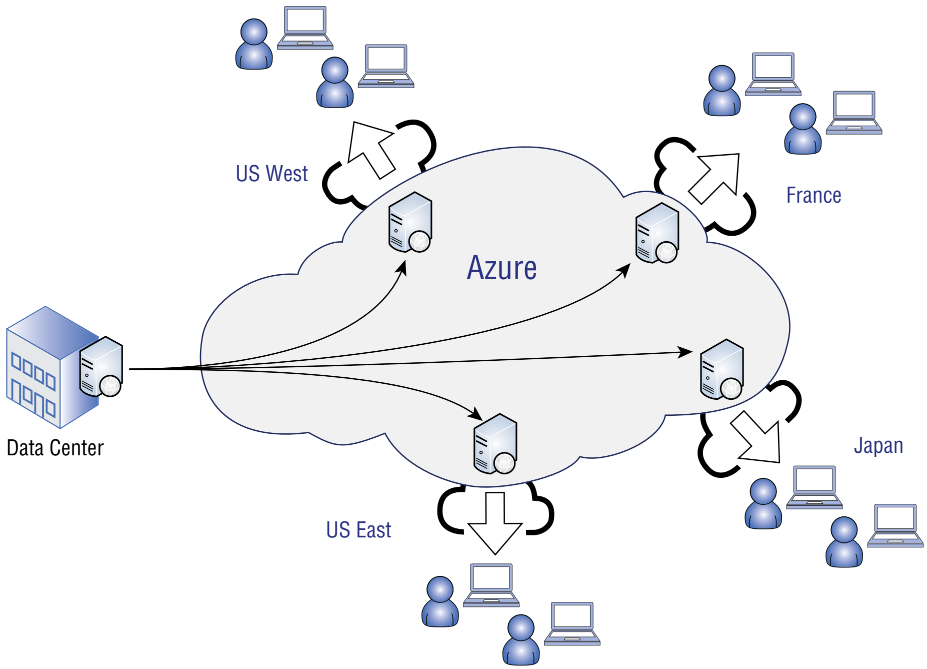


Content Delivery Networks

Azure Content Delivery Network (CDN) places web content across a distributed network of servers to make that content readily available to users based on their location. For example, if your organization is based in the United States but you have large video files that you need to make available to users in Switzerland, you could place those files on a CDN that has a point of presence (PoP) in Zurich or Geneva. When the users access those files, the files come from the cached copies in the CDN, rather from your servers in the United States. This reduces latency and improves performance. Figure 3.5 illustrates CDNs.

Each file has a time-to-live (TTL) property that determines when the file should be refreshed from the source to the cache. If the TTL has expired and a user requests the file, Azure CDN refreshes the data from the source to the cache and resets the TTL. This helps ensure that the file is up to date, but also helps reduce network traffic for files that do not change often, if at all. In the latter case, you could set a long TTL for the file to reduce how often it is copied to the cache.

FIGURE 3.5 A CDN places content close to users geographically.



Azure CDN supports CDN caching rules, compression, geofiltering, scalability, and several other features. For more details, visit `https://docs.microsoft.com/en-us/azure/cdn/cdn-overview`.

Summary

The services described in this chapter are the core networking services offered in Azure. Becoming familiar with these services will help you begin to understand how various Azure resources communicate with one another, how your organization can connect to the Azure network, and how to secure traffic between VNets in Azure and between your on-premises network and Azure.

This chapter covered the following concepts:

- **Networking addressing:** Devices on a network are assigned a network address, which uniquely identifies the device on the network and enables network traffic to be routed to and from the device. Subnets create virtual networks to segregate devices within an address space. When you create a resource in Azure, you specify the address segment in which it will reside and either assign it a static address or allow it to take a dynamic address.
- **Routing:** Routers move network traffic between network segments. They make it possible not only for public network segments to communicate, but also for private network segments to communicate with public network segments.

- **Domain Name Service (DNS):** DNS provides host-to-address resolution, enabling applications and services to determine the IP address associated with a hostname.
- **Virtual private network (VPN):** A VPN creates an encrypted tunnel between two private networks across a public network, enabling secure network traffic between the two networks. You can establish a VPN connection between Azure network segments, your on-premises network and Azure, or between specific hosts.
- **Load balancer:** A load balancer distributes traffic to a group of servers or services, enabling the load to be shared among them. Load balancing also enables fault tolerance by detecting failed resources and directing traffic away from them.
- **ExpressRoute:** Azure ExpressRoute enables you to establish a secure VPN connection between your on-premises network and Azure through a third-party provider, bypassing the Internet. ExpressRoute Direct enables you to connect your on-premises network directly to the Microsoft global network.
- **Content Delivery Network (CDN):** A CDN places content near users, enabling them to consume that content without pulling the data from a geographically distant server. CDNs reduce network traffic and latency.

Exam Essentials

Describe core resources available in Azure. You create VNets in Azure to segregate and organize hosts and services. Each VNet is scoped to a single subscription and region, but you can create multiple VNets. Virtual Network Peering enables you to connect VNets across regions.

The load-balancing services in Azure balance network traffic across multiple servers. Azure Load Balancer is used when you need to balance traffic based on IP address. Azure Application Gateway is used for regional load balancing of web applications, and Azure Front Door is intended for globally distributed web applications. Azure Traffic Manager is intended for regional or global DNS-based load balancing, but because it is DNS based it's not able to fail over as quickly as Front Door.

Virtual private networks (VPNs) enable you to connect two private networks using a tunnel through a public network such as the Internet. Use Azure VPN Gateway to establish VPN tunnels between Azure VNets and between Azure and your on-premises networks. VPN Gateway supports site-to-site, multi-site, point-to-site, and VNet-to-VNet connections. Azure ExpressRoute provides VPN connectivity between your on-premises network and Azure with higher possible speeds using third-party network providers. ExpressRoute Direct offers even higher speeds and connects directly to the Microsoft network rather than tunneling through the Internet.

Lastly, content delivery networks (CDNs) enable you to place content near where users are located, improving performance, minimizing network traffic, and reducing latency.

Review Questions

1. You are deploying a web application in Azure and need to distribute traffic based on a single public IP address to the virtual machines that are hosting the database. Which of the following best satisfies that requirement?

   A. Azure Application Gateway

   B. Azure Traffic Manager

   C. Azure Load Balancer

   D. Azure Front Door

2. Is the underlined portion of the following statement true, or does it need to be replaced with one of the other fragments that appear below?

   Your organization hosts its public website in Azure. You want to use URL path-based routing to accommodate processing for videos and images by sending traffic to server pools optimized for each content type. Your organization operates globally, and you also want to ensure the best possible performance regardless of where your consumers are in the world. You should use Application Gateway as a load-balancing solution to meet these requirements.

   A. Traffic Manager

   B. Front Door

   C. Azure Load Balancer

   D. No change is needed.

3. You are developing a solution in Azure that requires sending HTTPS traffic within a region to a specific endpoint based on the requested URL. Which of the following is the appropriate load-balancing service?

   A. Azure Application Gateway

   B. Azure Traffic Manager

   C. Azure Load Balancer

   D. Azure Front Door

4. Your organization is building a hybrid Azure environment where several on-premises services need to interact with resources in Azure, and vice versa, over a secure connection. You require high-speed connectivity through an encrypted tunnel across the Internet. The connection will be provided and managed by a third party. Which Azure service does this scenario describe?

   A. Azure Client VPN

   B. Azure VPN Gateway

   C. Azure ExpressRoute Direct

   D. Azure ExpressRoute

5. Your organization maintains two on-premises data centers named Alpha and Bravo, and you are considering moving some or all the resources hosted in those data centers to Azure. As part of an Azure proof of concept, you need to establish a connection to Azure from a server named vmtest01 in data center Alpha. Which VPN solution meets the requirement for minimum setup and cost?

A. An ExpressRoute connection between Alpha and Azure

B. A multi-site VPN connection between Alpha, Bravo, and Azure

C. A site-to-site VPN from vmtest01 to Azure

D. A point-to-site VPN from vmtest01 to Azure

6. You are an IT infrastructure manager for a large bank. You propose moving some of your IT infrastructure and services to Azure. You need to provide a secure, high-bandwidth connection from your primary data center to Azure, but the connection cannot traverse the Internet. Which of the following meets these requirements?

A. Azure VPN Gateway

B. Azure ExpressRoute Direct

C. Azure ExpressRoute

D. None of the above

7. Your global organization hosts an intranet that serves training content in the form of videos and large drawing files used by service personnel. These resources need to be available to users in the United States, Canada, the UK, and France with minimal network latency. Which of the following options meets these requirements with minimal cost?

A. Use Azure Content Delivery Network to host the files geographically close to your users.

B. Use VNet-to-VNet connections between regions to enable the documents and videos to flow rapidly between regions.

C. Use ExpressRoute to provide higher bandwidth for user connections.

D. None of the above.